

**IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE**

WAYMON BLEVINS and VICKIE LYNN BLEVINS, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

SPECIALTY NETWORKS, LLC,

Defendant.

Case No. _____

Jury Demand

Class Action

CLASS ACTION COMPLAINT

Plaintiffs Waymon Blevins (“Plaintiffs”), brings this Class Action Complaint against Defendant, Specialty Networks, LLC (“Defendant”), in their individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to their own actions and their counsels’ investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs brings this class action against Defendant for its failure to properly secure and safeguard Plaintiffs’ and other similarly situated current and former patients of Defendant’s clients’ (“Class Members,” defined *infra*) sensitive information, including protected health information (“PHI”) and other personally identifiable information (“PII”), including names, dates of birth, driver’s license numbers, and Social Security numbers, medical record numbers, treatment and condition information, diagnoses, medication, and health insurance information (“Private Information”). See Notice of Data Security Incident, attached hereto as Exhibit A.

2. Based in Chattanooga, Tennessee, Defendant¹ was founded in 2004 as an application services provider for Picture Archive and Communication Systems (PACS)². Over the course of that first year, Defendant grew to be a provider of radiology information systems (RIS), digital transcription services, and Enterprise Practice Management solutions (EPM) to its clients, which are medical facilities.³ Defendant currently has between 2-10 employees and 3 imaging center locations in Chattanooga, Tennessee and Ringgold, Georgia.⁴

3. Defendant received Plaintiffs and Class Members' Private Information in its provision of services to its clients for the benefit of Plaintiffs and Class Members.

4. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about August 15, 2024, Defendant announced that an unauthorized actor acquired certain data stored within its systems on or around December 11, 2023 ("Data Breach"). The Private Information of over thousands of individuals is believed to have been exposed by the Data Breach.

6. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This

¹ Defendant should not be confused with Ohio-based Specialty Networks, which was acquired by Cardinal Health in early 2024. *See* <https://radiologybusiness.com/topics/health-it/enterprise-imaging/radiology-information-systems-provider-reports-data-breach>.

² “[PACS is] a medical imaging technology that provides economical storage, retrieval, management, distribution, and presentation of medical images. PACS storage refers to the storage infrastructure dedicated to housing these medical images and related data within a healthcare facility.” <https://www.specialtynet.com/about>. According to Defendant, “PACS storage plays a crucial role in modern healthcare by facilitating the efficient management and accessibility of medical images, ultimately contributing to improved patient care and outcomes.” *Id.*

³ <https://www.linkedin.com/company/specialty-networks-llc/about/>.

⁴ *Id.*

unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its clients' patients' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

7. Plaintiffs brings this action on behalf of all persons whose Private Information was compromised because of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure its network containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal statutes.

8. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

9. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

10. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seeks to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

11. Plaintiffs were and was, at all times material hereto, are residents and citizens of South Pittsburg, Tennessee, where they intends to remain.

12. Defendant is a Tennessee limited liability company with its principal place of business located at 1604 Gunbarrel Road, Chattanooga, Tennessee 37421.

JURISDICTION AND VENUE

13. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. Upon information and belief, there are thousands of Class Members, many of whom reside outside the state of Tennessee and have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

14. This Court has general personal jurisdiction over Defendant because it is

headquartered in this District.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1331(b) because Defendant resides in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendant is subject to the Court's personal jurisdiction with respect to this action.

FACTUAL ALLEGATIONS

16. Plaintiffs provided their Private Information to Defendant in connection with services he received from their medical provider.

17. Because of Defendant's failure to implement reasonable, industry standard cybersecurity safeguards, Plaintiffs' Social Security number, driver's license, date of birth, and highly sensitive health information—including diagnoses and medication—are now in the hands of identity thieves.

18. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

19. Upon information and belief, Defendant made promises and representations to Plaintiffs and Class Members that their Private Information would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

20. Plaintiffs' and Class Members' Private Information was provided to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

21. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

22. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's Private Information safe and confidential.

23. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

24. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

25. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

The Data Breach

26. On August 15, 2024, Defendant announced that an unauthorized actor acquired certain data stored within its systems.

27. The Notice of Data Security Incident sent to Plaintiffs and Class Members states:

What Happened?

On December 18, 2023, Specialty Networks became aware of unusual activity in our network. Upon discovering this activity, we immediately took steps to secure the network and engaged a digital forensics and incident response firm to conduct an investigation to determine what happened and whether any data within our environment may have been impacted. The investigation revealed that on or about December 11, 2023, an unauthorized actor acquired certain data stored within our systems. Specialty Networks then undertook a comprehensive review of the potentially impacted data and, on May 31, 2024, determined that your personal and/or protected health information may have been involved. We then worked to

verify the affected information and mailing addresses for impacted individuals to ensure we had the most up to date contact information...

What Information Was Involved?

Your personal and protected health information that may have been involved in the incident included: name, date of birth, driver's license number, Social Security number, medical record number, treatment and condition information, diagnoses, medications, and health insurance information.⁵

28. Defendant further states that upon discovering the incident, it "took the steps described above and implemented additional measures to enhance our network security and minimize the risk of a similar incident occurring in the future."⁶

29. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

30. The attacker accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

31. Plaintiffs further believes their Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

**Defendant Acquires, Collects, and Stores
the Private Information of Plaintiffs and Class Members**

32. Defendant derives a substantial economic benefit from substantial economic benefit from providing services to its clients (i.e., Plaintiffs' and Class Members' medical

⁵ See Notice of Data Security Incident provided to Plaintiffs, a true and correct copy of which is attached hereto as **Exhibit A**.

⁶ *Id.*

providers), and as a part of providing those services, Defendant retains and stores Plaintiffs' and Class Members' Private Information.

33. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the Private Information from disclosure.

34. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

35. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

36. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

37. Upon information and belief, Defendant made promises to Plaintiffs and Class Members to maintain and protect Plaintiffs' and Class Members' Private Information, demonstrating an understanding of the importance of securing Private Information.

38. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of Private Information are Particularly Susceptible to Cyber Attacks.

39. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

40. Data thieves regularly target institutions like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

41. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.⁷

42. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information it collected and maintained would be targeted by cybercriminals.

43. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

44. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

45. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially thousands of individuals'

⁷ See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (<https://notified.idtheftcenter.org/s/>), at 6.

detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

46. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

47. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly PHI—fraudulent use of that information and damage to victims may continue for years.

Value of Personally Identifiable Information

48. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."⁸ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."⁹

49. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹⁰

⁸ 17 C.F.R. § 248.201 (2013).

⁹ *Id.*

¹⁰ *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS, Oct. 16, 2019, <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

50. For example, Private Information can be sold at a price ranging from \$40 to \$200.¹¹

Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹²

51. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”¹³

52. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient’s complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a “cyber black market” exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the health care industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

53. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.¹⁴ Indeed, during 2019 alone, over 41 million health care records were exposed, stolen, or unlawfully disclosed in 505 data breaches.¹⁵ In short, these sorts of data breaches are

¹¹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

¹² *In the Dark*, VPNOVERVIEW, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

¹³ *Medical I.D. Theft*, EFraudPrevention <https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected>.

¹⁴ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/>.

¹⁵ <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/>.

increasingly common, especially among health care systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.¹⁶

54. According to account monitoring company LogDog, medical data sells for \$50 and up on the dark web.¹⁷

55. “Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy Forum. “Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief’s activities.”¹⁸

56. A study by Experian found that the average cost of medical identity theft is “about \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for health care they did not receive to restore coverage.¹⁹ Almost half of medical identity theft victims lose their health care coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.²⁰

57. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

¹⁶ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/>.

¹⁷ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>.

¹⁸ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>.

¹⁹ See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>.

²⁰ *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>.

breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—PHI, names, and dates of birth—is impossible to “close” and difficult, if not impossible, to change.

58. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”²¹

59. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

60. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²²

Defendant Failed to Comply with FTC Guidelines.

61. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for

²¹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

²² *Report to Congressional Requesters*, GAO, at 29 (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf>.

consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

62. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

63. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

64. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

65. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security

practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

66. Defendant was at all times fully aware of its obligation to protect the Private Information of consumers under the FTCA yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

67. Defendant's failure is even more clear given the timeline alleged here. Defendant's investigation revealed that the attack occurred on December 11, 2023, but it did not discover the activity until December 18, 2023. Given that Defendant did not identify the malicious activity until a week after it began, Defendant likely failed to implement the required monitoring, logging, and alerting safeguards that are a part of all reasonable, industry standard cybersecurity programs.

68. Still further, Defendant did not notify class members, including Plaintiffs, until some 9 months after the Breach, which flies in the face of Defendant's statutory notification requirements and shows that Defendant's cybersecurity incident response plans were severely below standard.

Defendant Failed to Comply with HIPAA Guidelines.

69. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health

Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

70. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

71. HIPAA’s Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

72. HIPAA’s Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

73. HIPAA requires “comply[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

74. “Electronic protected health information” is “individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R. § 160.103.

75. HIPAA’s Security Rule requires defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

76. HIPAA also requires Defendant to “review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

77. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

78. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and in no case later than 60 days following discovery of the breach.”

79. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

80. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the

covered entity or its business associate. *See 45 C.F.R. § 164.530(f).*

81. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See 45 C.F.R. §§ 164.302-164.318.* For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.

82. Defendant was at all times fully aware of its HIPAA obligations to protect the Private Information of consumers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant’s conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

83. Here again, Defendant’s failure is even more clear given the timeline alleged here. Defendant’s investigation revealed that the attack occurred on December 11, 2023, but it did not discover the activity until December 18, 2023. Given that Defendant did not identify the malicious activity until a week after it began, Defendant likely failed to implement the required monitoring, logging, and alerting safeguards that are a part of all reasonable, industry standard cybersecurity

programs.

84. Still further, Defendant did not notify class members, including Plaintiffs, until some 9 months after the Breach, which flies in the face of Defendant's statutory notification requirements and shows that Defendant's cybersecurity incident response plans were severely below standard.

Defendant Failed to Comply with Industry Standards.

85. Experts studying cybersecurity routinely identify institutions that store Private Information like Defendant as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

86. Some industry best practices that should be implemented by institutions dealing with sensitive Private Information, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

87. Other best cybersecurity practices that are standard at large institutions that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

88. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation

PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

89. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Defendant Breached Its Duty to Safeguard Plaintiffs' and Class Members' Private Information.

90. In addition to its obligations under federal laws, Defendant owed duties to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

91. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect consumers' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to adhere to industry standards for cybersecurity as discussed above; and

e. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

92. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems, including its employees' email accounts, which contained unsecured and unencrypted Private Information.

93. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

Common Injuries & Damages

94. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

The Data Breach Increases Victims' Risk of Identity Theft.

95. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

96. The unencrypted Private Information of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

97. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

98. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

99. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means

such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

100. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Full” packages.²³

101. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

102. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

²³ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm>.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

103. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

104. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

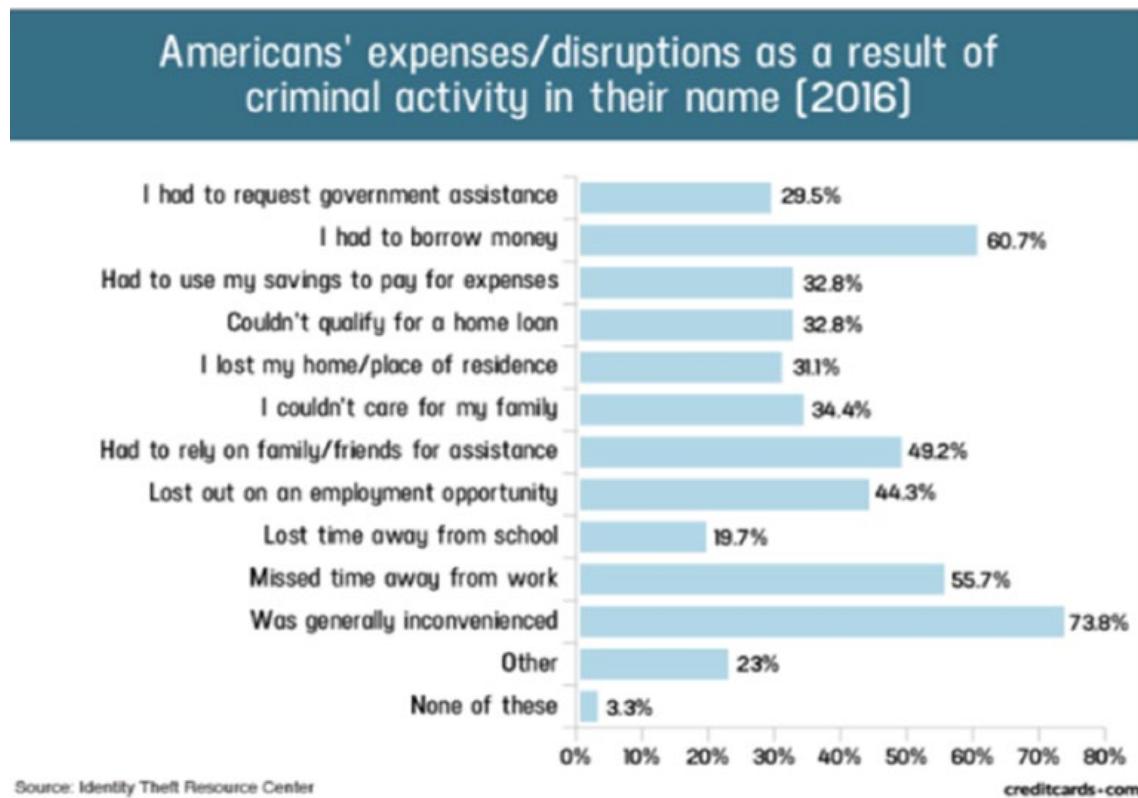
105. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁴

106. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended

²⁴ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁵

107. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:²⁶



Diminution of Value of Private Information

108. PII and PHI are valuable property rights.²⁷ Their value is axiomatic, considering

²⁵ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>.

²⁶ Jason Steele, "Credit Card and ID Theft Statistics," Oct. 24, 2017, <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>.

²⁷ See, e.g., Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that Private Information has considerable market value.

109. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly \$200 billion.²⁸

110. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{29,30}

111. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³¹

112. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”

113. As a result of the Data Breach, Plaintiffs’ and Class Members’ Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

²⁸ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

²⁹ <https://datacoup.com/>.

³⁰ <https://digi.me/what-is-digime/>.

³¹ Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html>.

114. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if their data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

115. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its network, amounting to likely thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

116. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary.

117. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes.

118. Such fraud may go undetected for years; consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

119. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect

Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Plaintiffs' Experience

120. Plaintiffs provided their Private Information to Defendant in connection with medical services he received from their medical provider.

121. At the time of the Data Breach, Defendant retained Plaintiffs' Private Information in its system.

122. Plaintiffs' Private Information was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the Private Information.

123. Plaintiffs takes reasonable measures to protect their Private Information. He has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

124. Plaintiffs stores any documents containing their Private Information in a safe and secure location and diligently chooses unique usernames and passwords for their online accounts.

125. Plaintiffs and Class Members have been injured by the compromise of their Private Information.

126. Because of the Data Breach, Plaintiffs has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

127. Plaintiffs also suffered actual injury in the form of damages to and diminution in

the value of their Private Information—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and because of the Data Breach.

128. Plaintiffs suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of their privacy. For one thing, he has noticed a spike in spam and scam calls and emails since the Data Breach.

129. Plaintiffs has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information, especially their name and PHI, being placed in the hands of criminals.

130. Defendant obtained and continues to maintain Plaintiffs' Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiffs' Private Information was compromised and disclosed as a result of the Data Breach.

131. As a result of the Data Breach, Plaintiffs anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiffs is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

132. Pursuant to Federal Rules of Civil Procedure 12(b)(2), 23(b)(3), and 23(c)(4), Plaintiffs brings this action on behalf of themselves and on behalf of all members of the proposed class defined as:

All individuals residing in the United States whose Private Information was compromised in the Data Breach (“Class”).

133. Excluded from the Class are the following individuals and/or entities: Defendant

and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

134. Plaintiffs reserves the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

135. The proposed Class meets the criteria certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

136. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believes the proposed Class includes thousands of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendant's records.

137. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant engaged in the conduct alleged herein;
- b. Whether Defendant's conduct violated the FTCA;
- c. When Defendant learned of the Data Breach;
- d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

- e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- f. Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;
- g. Whether Defendant owed duties to Class Members to safeguard their Private Information;
- h. Whether Defendant breached their duties to Class Members to safeguard their Private Information;
- i. Whether hackers obtained Class Members' Private Information via the Data Breach;
- j. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- k. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- l. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;
- m. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;
- n. Whether Defendant's conduct was negligent;
- o. Whether Defendant breached contracts it had with its clients, which were made expressly for the benefit of Plaintiffs and Class Members;
- p. Whether Defendant were unjustly enriched;
- q. Whether Plaintiffs and Class Members are entitled to damages;

r. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

138. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiffs is advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

139. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

140. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members. For example, all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

141. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is

superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

142. Class certification is also appropriate under Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

143. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

CLAIMS FOR RELIEF

COUNT I **NEGLIGENCE** **(On Behalf of Plaintiffs and the Class)**

144. Plaintiffs incorporates the above allegations as if fully set forth herein.

145. Plaintiffs and Class Members provided their non-public Private Information to Defendant in connection with and as a condition of obtaining medical services from Defendant's clients.

146. Defendant had full knowledge of the sensitivity of the Private Information and the

types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

147. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

148. Defendant had duties to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

149. Defendant’s duty to use reasonable security measures under HIPAA required Defendant to “reasonably protect” confidential data from “any intentional or unintentional use or disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1). Some or all of the health care and/or medical information at issue in this case constitutes “protected health information” within the meaning of HIPAA.

150. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

151. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

152. Defendant had and continues to have duties to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendant’s possession might have been

compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

153. Defendant breached its duties, pursuant to the FTCA, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems, including by failing to implement reasonable monitoring, logging, and alerting systems such as EDR/XDR and a centralized security event management system;
- c. Allowing unauthorized access to Class Members' Private Information;
- d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- e. Failing to remove Plaintiffs' and Class Members' Private Information it was no longer required to retain pursuant to regulations; and
- f. Failing to implement reasonable incident response, business continuity, and disaster recovery plans that would have enable Defendant to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

154. Defendant's conduct was particularly unreasonable given the nature and amount of

Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

155. Defendant's violation of federal statutes also constitutes negligence *per se*. Specifically, as described herein, Defendant has violated the FTCA and HIPAA.

156. Plaintiffs and Class Members were within the class of persons the FTCA and HIPPA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

157. Defendant has admitted that the Private Information of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

158. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiffs and Class Members, the Private Information of Plaintiffs and Class Members would not have been compromised.

159. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

160. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the

Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

161. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

162. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

163. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

164. Given Defendant's failures to implement the proper systems, as defined above, even knowing the ubiquity of the threat of data breaches in the healthcare industry, Defendant's decision not to invest enough resources in its cyber defenses amounts to gross negligence.

COUNT II
Breach of Third Party Beneficiary Contract
(On Behalf of Plaintiffs and the Class)

165. Plaintiffs incorporates the above allegations as if fully set forth herein.

166. Upon information and belief, Defendant entered into virtually identical contracts with its clients to provide services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

167. Such contracts were made expressly for the benefit of Plaintiffs and Class Members, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

168. Defendant knew that if it were to breach these contracts with its clients, Plaintiffs and the Class would be harmed.

169. Defendant breached its contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when Defendant failed to use reasonable data security measures that could have prevented the Data Breach.

170. As foreseen, Plaintiffs and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

171. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost

time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

172. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

173. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

174. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

175. Plaintiffs incorporates the above allegations as if fully set forth herein.

176. Plaintiffs brings this claim in the alternative to their breach of third-party beneficiary contract claim above.

177. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Defendant

should have provided adequate data security for Plaintiffs and Class Members.

178. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as a necessary part of their receiving services from Defendant's clients. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

179. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

180. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

181. Defendant, however, failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

182. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

183. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

184. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to

Defendant.

185. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

186. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

187. Plaintiffs and Class Members have no adequate remedy at law.

188. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

189. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

190. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

- ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;
- v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

- viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- ix. requiring Defendant to conduct regular database scanning and securing checks;
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
- xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xii. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

- xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
- xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

E. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: August 20, 2024.

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (TN BPR # 23045)
Grayson Wells (TN BPR # 039658)
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwellss@stranchlaw.com

Jeff Ostrow (*pro hac vice* forthcoming)
Kristen Lake Cardoso (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Ste. 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
ostrow@kolawyers.com
cardoso@kolawyers.com

Counsel for Plaintiffs and the Putative Class